BURSOR & FISHER, P.A.
L. Timothy Fisher (State Bar No. 191626)
Joel D. Smith (State Bar No. 244902)
1990 North California Boulevard, Suite 940
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
E-Mail: ltfisher@bursor.com
jsmith@bursor.com

BURSOR & FISHER, P.A.
Alec M. Leslie (*Pro Hac Vice*)
Max S. Roberts (*Pro Hac Vice*)
888 Seventh Avenue, Third Floor
New York, NY 10019
Telephone: (646) 837-7150
Facsimile: (212) 989-9163
E-Mail: aleslie@bursor.com
mroberts@bursor.com

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

AUDRA GRAHAM and STACY MOISE, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

NOOM, INC. and FULLSTORY, INC.,

Defendants.

Case No. 3:20-cv-06903-LB

SECOND AMENDED CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiffs Audra Graham and Stacy Moise ("Plaintiffs"), individually and on behalf of all others similarly situated, by and through their attorneys, make the following allegations pursuant to the investigation of their counsel and based upon information and belief, except as to allegations specifically pertaining to themselves and their counsel, which are based on personal knowledge.

NATURE OF THE ACTION

1. This is a class action suit brought against Defendants Noom, Inc. ("Noom") and FullStory, Inc. ("FullStory") (collectively, "Defendants") for wiretapping the electronic communications of visitors to Defendant Noom's website, Noom.com (the "Website").[1] The wiretaps, which are embedded in the computer code on the Website, are used by Defendants to secretly observe and record website visitors' keystrokes, mouse clicks,[2] and other electronic communications, including the entry of Personally Identifiable Information ("PII") and Protected Health Information ("PHI"), in real time. By doing so, Defendants have violated the California Invasion of Privacy Act ("CIPA"), Cal. Penal Code §§ 631 and 635, and invaded Plaintiffs' and class members' privacy rights in violation of the California Constitution.

2. On November 17, 2019, Ms. Graham visited the Website. Likewise, on June 23, 2020, Ms. Moise visited the Website. During the visits, FullStory—as enabled by Noom—captured, stored, and analyzed Plaintiffs' electronic communications in real time, and used the intercepted data to attempt to learn their e-mail, height, weight, age range, gender, medical conditions, and other PII and PHI.

3. Plaintiffs bring this action on behalf of themselves and a class of all persons whose electronic communications were intercepted through the use of Defendants' wiretap on the Website.

THE PARTIES

4. Plaintiff Audra Graham is a California citizen and resident who lives in Oakland, California. Ms. Graham is domiciled and intends to remain in California. On November 17, 2019,

[1] NOOM, https://www.noom.com/#/ (last accessed Sept. 9, 2020).

[2] As used herein, the term "mouse clicks" also refers to "touch gestures" such as the "tap," "swipe," and similar gestures used on touchscreen devices.

prior to the filing of this lawsuit, Ms. Graham browsed the Website on her computer while investigating Defendant Noom's diet offerings. Ms. Graham was in Oakland when she visited the Website. During the visit, Ms. Graham filled out portions of the form on Noom's website—thus providing at least some of the personal and medical information detailed below—as well as performed other behaviors like scrolling, clicking, and typing. During the visit, Ms. Graham's keystrokes, mouse clicks, and other electronic communications—including the entry of her e-mail, height, weight, age range, gender, medical conditions, and other PII and PHI—were intercepted in real time by Defendant FullStory and disclosed to Defendant FullStory through the wiretap. Ms. Graham was unaware at the time that her keystrokes, mouse clicks, and other electronic communications, including the information described above, were being intercepted in real-time and would be disclosed to FullStory, nor did Ms. Graham consent to the same.

5. Plaintiff Stacy Moise is a California citizen and resident who lives in Pasadena, California. Ms. Moise is domiciled and intends to remain in California. On June 23, 2020, prior to the filing of this lawsuit, Ms. Moise browsed the Website on her cell phone while investigating Defendant Noom's diet offerings. Ms. Moise was in Canyon Country, California when she visited the Website. During the visit, Ms. Moise filled out portions of the form on Noom's website—thus providing at least some of the personal and medical information detailed below—as well as performed other behaviors like scrolling, clicking, and typing. During the visit, Ms. Moise's keystrokes, mouse clicks, and other electronic communications—including the entry of her e-mail, height, weight, age range, gender, medical conditions, and other PII and PHI—were intercepted in real time by Defendant FullStory and disclosed to Defendant FullStory through the wiretap. Ms. Moise was unaware at the time that her keystrokes, mouse clicks, and other electronic communications, including the information described above, were being intercepted in real-time and would be disclosed to FullStory, nor did Ms. Moise consent to the same. In fact, Ms. Moise never signed up to use Defendant Noom's services.

6. Defendant Noom, Inc. is a Delaware limited liability company with its principal place of business at 229 West 28th Street, 9th Floor, New York, New York 10001.

7. Upon information and belief, the Website was visited over five million times in August 2020 alone.[3]

8. Noom does business throughout California and the entire United States.

9. Noom actively advertises its services in California and uses these advertisements to lure consumers to the Website.

10. Noom owns and operates the Website.

11. Defendant FullStory is a Delaware corporation with its principal place of business at 1745 Peachtree Street Northwest, Suite G, Atlanta, Georgia 30309.

12. FullStory is a marketing software-as-a-service ("SaaS") company.

13. FullStory provides a feature called "Session Replay," which is at issue here and described more fully below. At all relevant times here, Noom has used FullStory's "Session Replay" product on its website.

JURISDICTION AND VENUE

14. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2)(A) because this case is a class action where the aggregate claims of all members of the proposed class are in excess of $5,000,000.00, exclusive of interest and costs, and at least one member of the proposed class is citizen of state different from at least one Defendant.

15. This Court has personal jurisdiction over Defendants because each of the Defendants have purposefully availed themselves of the laws and benefits of doing business in this State, and Plaintiffs' claims arise out of each of the Defendants' forum-related activities. Furthermore, a substantial portion of the events giving rise to Plaintiffs' claims occurred in this District.

16. Both Defendants also purposefully directed their activities to California, and the wiretapping at issue here arises from or relates to Defendants' activities. As alleged more fully below, Defendants intentionally installed the wiretap at issue here on Noom's Website. Defendant FullStory purposefully intercepted electronic transmissions from users of Noom's website, and Noom purposefully aided and abetted FullStory's conduct. The conduct also was expressly aimed

[3] https://www.similarweb.com/website/noom.com/.

at California residents. California is the largest market in the United States—indeed, if California were its own nation, California would have the fifth largest economy in the world. The Website operates in both English and Spanish, the first and second most common languages spoken by California residents. Defendants knew that a significant number of Californians would visit Noom's website, because they form a significant portion of Noom's customer base. Indeed, as alleged further, FullStory wiretaps geolocation information, and therefore knows it is wiretapping users in California. By intercepting the transmissions of Noom website users, Defendants targeted their wrongful conduct at customers, some of whom Defendants knew, at least constructively, were residents of California. It was foreseeable that Defendants' interceptions and wiretapping would harm Plaintiffs and similarly-situated individuals, and that at least some of this harm would occur in California—where Defendants knew many customers and prospective customers resided.

17. Pursuant to 28 U.S.C. § 1391, this Court is the proper venue for this action because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District.

STATEMENT OF FACTS

I. Overview Of The Wiretaps

18. Defendant FullStory develops a software of the same name. One of FullStory's features is called "Session Replay."

19. FullStory says that "Session replay tools capture things like mouse movements, clicks, typing, scrolling, swiping, tapping, etc." on a given website.

20. Session replay technologies work by using "embedded snippets of code … [that] watch and record a visitor's every move on a website, in real time."[4]

21. FullStory touts that Session Replay relies on real video of a user's interactions with a website, or, in other words, a "recorded session."[5]

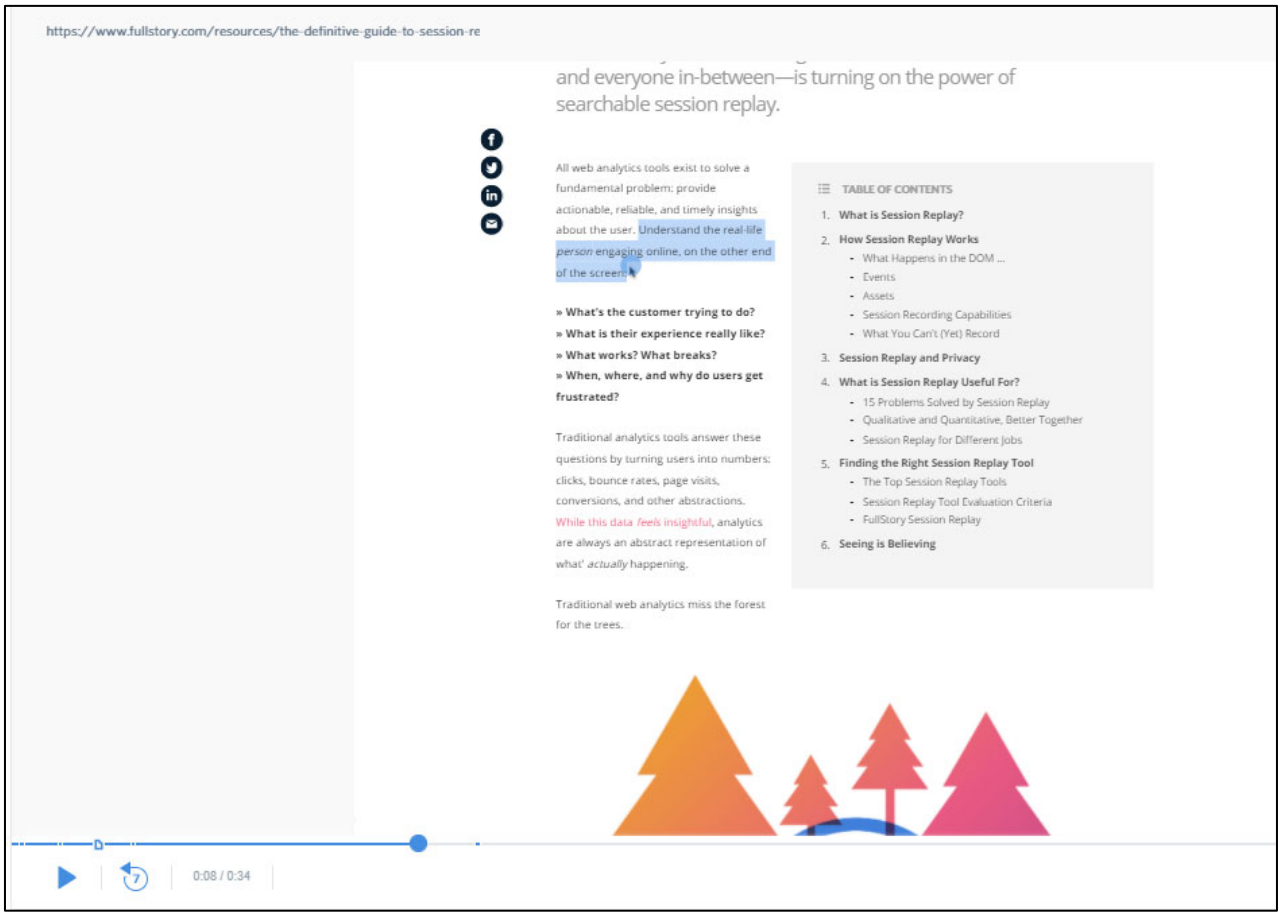
22. FullStory also states that it allows website owners to "literally visualize what users

[4] Tomas Foltyn, *What's the Deal with Session-Replay Scripts?*, WELIVESECURITY, Apr. 20, 2018, https://www.welivesecurity.com/2018/04/20/whats-deal-session-replay-scripts/.

[5] https://www.fullstory.com/resources/the-definitive-guide-to-session-replay/.

are experiencing, like watching a television show on a DVR."

23. To demonstrate how Session Replay works, FullStory displays the "recorded session of a fictional user interacting with th[e] [Session Replay] Guide":

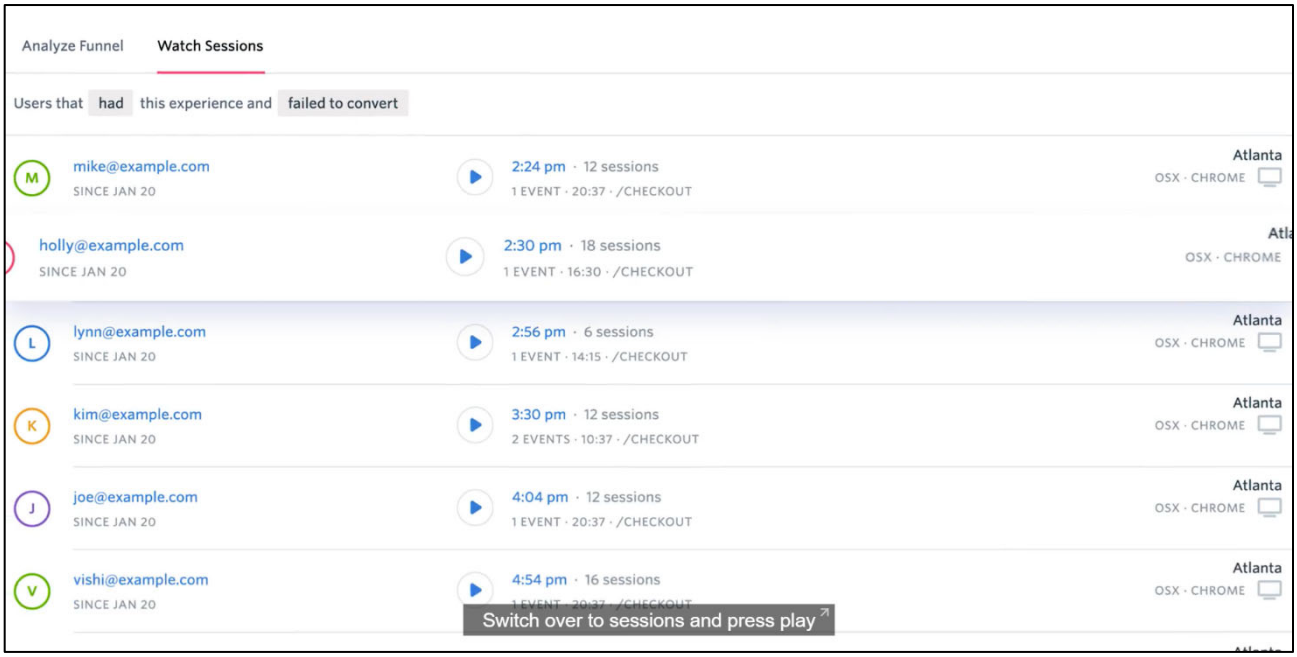


24. FullStory describes the above video as follows:

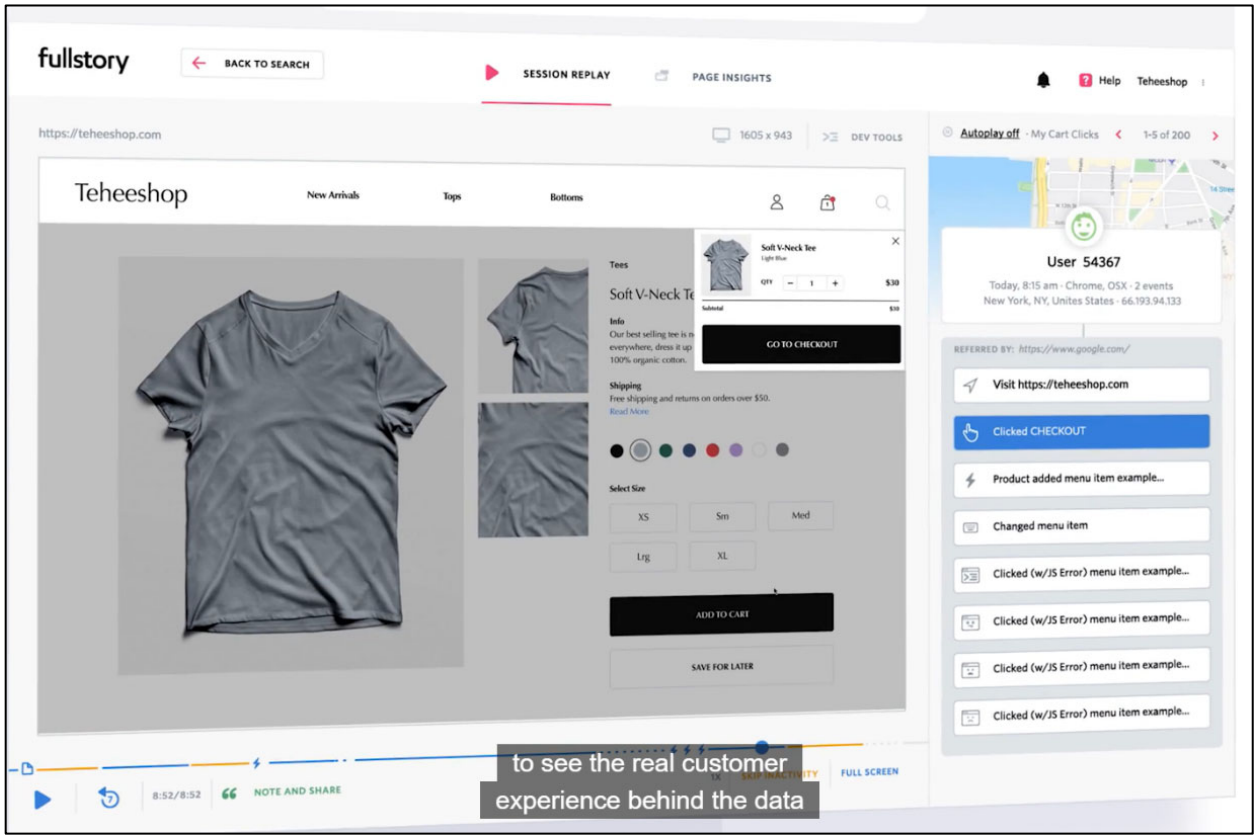
> Here you can watch a FullStory session replay of a user—Daniel Falko—flipping through *The Definitive Guide to Session Replay*. **Notice how you can see interactions, mouse movements, clicks, interactions with overlays, and more**—and everything is listed in order in a stream at the right side of the replay. This is what a session replay looks like in the FullStory app.[6]

25. FullStory's promotional video shows the behind-the-scenes features of the software. First, FullStory lets you view a list of users who visited the website, as well as the time they spent on the website:

[6] https://www.FullStory.com/resources/the-definitive-guide-to-session-replay/#finding-the-right-session-replay-tool (emphasis added).



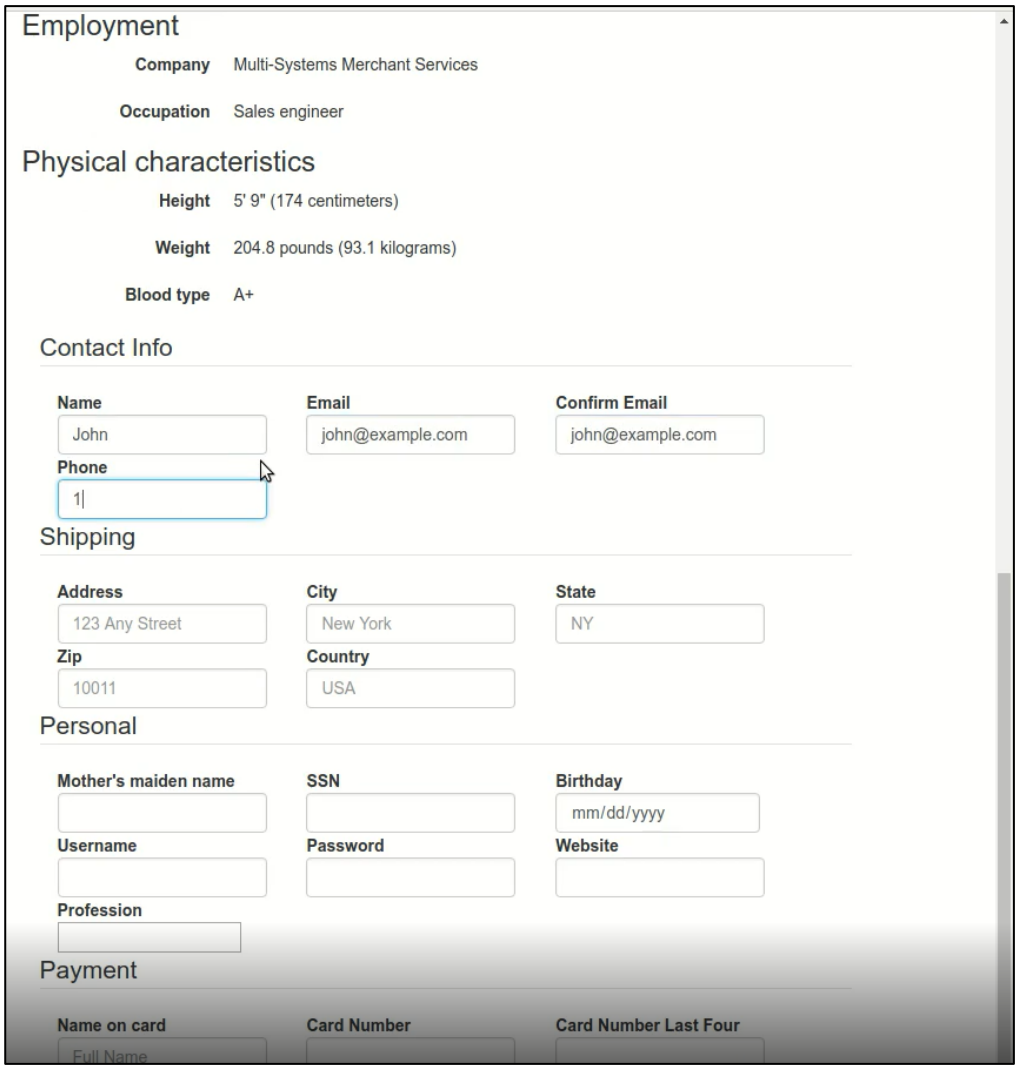
26. Upon clicking one of these "sessions," FullStory lets a company view the video of a user's interaction with a website, including mouse movements, clicks, interactions with overlays, keystrokes, geographic location, IP address, and more "to see the real customer experience behind the data":



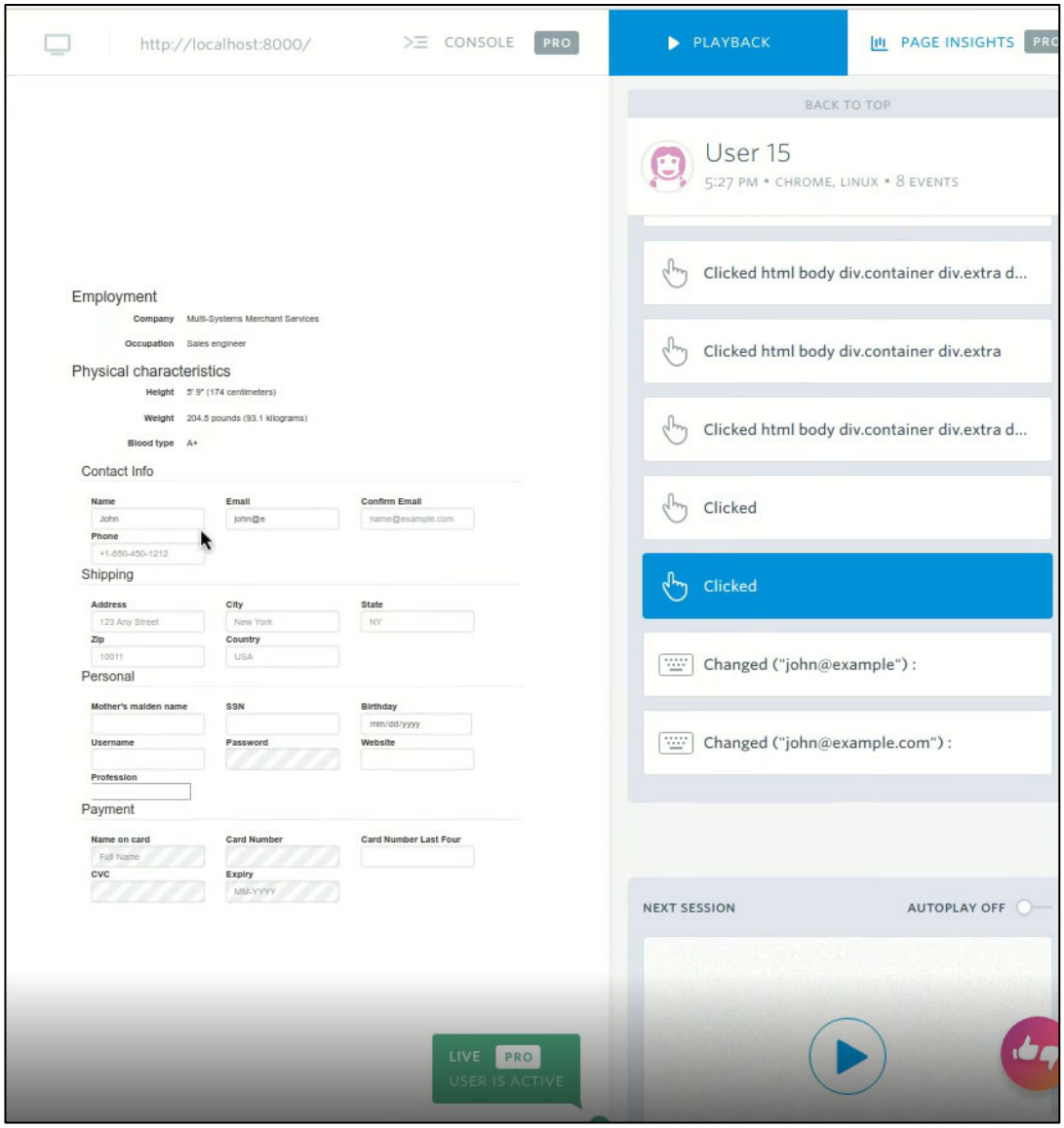
27. FullStory instructs prospective partners that "[t]he first step toward recording all in-browser interactions and making them available for pixel-perfect playback is deploying FullStory's recording JavaScript snippet. Simply paste the snippet into the <head> element via your Content Management System (CMS), via your online store platform, or via your application's code."

28. Upon pasting this snippet of code on a website, FullStory is able to record the keystrokes, mouse clicks, data entry, and other electronic communications of visitors to websites where the code is installed. It also allows FullStory to track the amount of time spent on the website, geographic location of the visitor, and other information described above.

29. A 2017 study by Princeton University researchers shows this process in action. In the first screenshot below, a mock user visits a website and enters information:



30. In the second screenshot, one can see FullStory's dashboard.[7] The information is simultaneously recorded by FullStory, and less than a second later, the user's actions can be seen in FullStory's recording:



31. FullStory's recording is not limited to desktop website, but also mobile websites and mobile applications.[8]

32. FullStory not only records users' electronic communications in real time for later

[7] These two images are displayed side-by-side in the study. Plaintiffs have separated the two images so that they can be made larger for clarity.

[8] https://www.fullstory.com/mobile-apps/.

viewing, but also allows websites to monitor them *live*. "For sessions that are actively recording and we [i.e., Defendant FullStory] are still receiving events from a user (meaning the last page in their session is still open), you'll see a 'Go Live' button at the end of the playback bar. Once you click on the button, you'll essentially be riding along in near real time with the user with no need to refresh the playback."

33. FullStory's code is not a cookie at all, much less a run-of-the-mill cookie. Common cookies that consumers might be familiar with do not engage in session recording or all of the features described above. FullStory's code does far more than simply track where a visitor went on the internet, and its functionality is not limited to aggregate data. Rather, as a 2017 study by Princeton University researchers—which specifically examined FullStory—noted, "unlike typical analytics services that provide aggregate statistics, these scripts are intended for the recording and playback of individual browsing sessions, as if someone is looking over your shoulder."

34. Technology like FullStory's Session Replay feature is not only highly intrusive, but dangerous. The 2017 study by Princeton University researchers found that session recording technologies were collecting sensitive user information such as passwords and credit card numbers. The research notes that this wasn't simply the result of a bug, but rather insecure practices. Thus, session recording technologies such as FullStory's can leave users vulnerable to data leaks and the harm resulting therefrom.

35. On its website, FullStory says its software "is a new technology." Hence, it is not ubiquitous, routine Internet activity. The Internet functioned for many years without session recording technology, and the Internet can and will continue to operate just fine without session recording technology.

36. FullStory's business model involves entering into voluntary partnerships with various companies and providing their software to their partners.

37. One of FullStory's partners is Defendant Noom.

38. Noom knows that FullStory's software captures the keystrokes, mouse clicks and other communications of visitors to its website, and pays FullStory to supply that information.

39. Pursuant to an agreement with FullStory, Noom enabled FullStory wrongful acts by voluntarily embedding FullStory's software code on the Website. This allowed FullStory to surreptitiously collect interactions between Noom and website users.

40. As currently deployed, FullStory's software, as employed by Noom, functions as a wiretap.

II. FullStory Did More Than Just Provide A Recording Device To Noom: It Was An Active Participant In The Wiretapping.

41. FullStory's patent states that, unlike older systems, FullStory's software actually transmits consumers' data to FullStory for storage and analysis:

> Because console logs are generated by the browser on the user device, the data of the console logs [logs that provide information about specific actions a user took] is generally not reported to a remote server, *absent the use of the present technology*. Instead, in prior systems, the data of the console logs remain local to the user device, and therefore is not used in the manner discussed throughout this document.

Synchronized Console Data and User Interface Playback, Patent No. 10,965,766, at 6:50-55 (Mar. 30, 2021) (emphasis added).

42. When the website user's communications are transmitted to Noom's Website, FullStory records the website user's interactions locally in the user's browser in real time, and then transmits that information to FullStory's recording servers every few seconds. FullStory then makes the information available to its clients. *See also* Patent No. 10,965,766, at 9:24-29 ("[T]he event data can include session replay data that is obtained and stored, and then used to generate playback data that presents visual changes to user interfaces during the user session and other activity (e.g. mouse movements) that occurred during the user session."); *id.* at 10:31-32 ("The event data can be transmitted to the evaluation apparatus in one or more data transmissions.").

43. FullStory not only captures user interactions with a website, it analyzes them itself. At the base level, FullStory analyzes data in order to index it for its clients to search through recordings. *See*, *e.g.*, *Evaluation of Interactions with a User Interface*, Patent No. 10,838,571, at 16:41-46 (Nov. 17, 2020) ("In some implementations, the session activity data and/or playback data are indexed to facilitate searches for specified user interactions or events. For example, multidimensional indexing can be performed so that user sessions during which a given user

interaction (or other event) occurred can be identified for a publisher."); *id.* at 25:48-50 ("In some implementations, the publisher specified data can be indexed according to each user session with which the user identified is associated.").

44. In addition, FullStory's software "can analyze the event data to identify specified events and obtain contextual data related to the events. For example, the event processing apparatus can identify the user click of event 1, and analyze the event data to obtain contextual data related to that user click." Patent No. 10,838,571, at 13:62-67.

45. FullStory's analysis goes beyond this, however. For instance, FullStory can combine its own session replay information with other information obtained by website owners to provide a comprehensive log of user activities. "For example, a publisher [website owner] could submit a request for session information related to users that had a historical purchase value of less than $X, and terminated their user session after interacting with a specified user interface element, and replay sessions returned in response to the request." Patent No. 10,838,571, at 25:15-21.

46. More intrusively, FullStory can obtain data from other third-party applications and combine that data with its session replays:

> In some implementations, the publisher specified data are obtained during a given user session, and are associated with a user of the user session. For example, assume that a user identifier (e.g. a cookie identifier)[9] is detected by the publisher during a given user session. In this example, code in the publisher's resource (or native application) can request additional data corresponding to the user identifier from a database of the publisher. For example, historical purchase information, download information, or other information that the publisher has stored in association with the user identified *can be obtained from the publisher's data store and uploaded as part of the event data*.

Patent No. 10,838,571, at 25:30-42 (emphasis added). Using this data, FullStory can, for example, display the "state of the user (e.g. the value of their shopping cart)" throughout the replay. Patent No. 10,838,571, at 25:63-26:3. This same process thus also allows FullStory to identify individuals who use websites by aggregating data from multiple sources.

47. FullStory states that when it comes to web analytics, "FullStory does the work for

[9] Of note, FullStory's patent here specifically distinguishes its software from a cookie, or refers to cookies as separate software from FullStory's.

you, gathering usability data automatically and comprehensively."

48. FullStory's standard Partner Terms and Conditions with its website-owner customers also confirms that Defendant FullStory has access to the communications recorded by its software.

- Website owners must "grant[] FullStory a non-exclusive, royalty-free license to access and use Customer Data in order to provide the services to Customer and as necessary to monitor and improve the Services."
- FullStory is permitted to use and disclose anonymized data for product improvement.
- If website owners want to remove certain sensitive data captured by the software, the website owner cannot do so on its own. Instead, the website owner must notify FullStory and ask it to locate and delete the data.

49. For these reasons, FullStory's software is also not a simple tape recorder or screen recording software. Tape recorders or screen recorders do not allow the company that manufacturers or develops the product or software to also have access to the recordings. Nor do such products analyze data to search for specific words in recordings, or combine data from other sources with the recordings. FullStory's software, however, does both of these things. It not only has access to interactions between consumers and websites—interactions for which FullStory was not the intended recipient—but also can combine those recordings with other data it obtains from website owners, giving it a comprehensive picture of any website user.

III. FullStory—As Enabled By Noom—Wiretapped Plaintiffs' Electronic Communications

50. On November 17, 2019, Ms. Graham visited the Website. She filled out portions of the form on Noom's website—thus providing at least some of the personal and medical information detailed below—as well as performed other behaviors like scrolling, clicking, and typing.

51. Likewise, on June 23, 2020, Ms. Moise visited the Website. She filled out portions of the form on Noom's website—thus providing at least some of the personal and medical information detailed below—as well as performed other behaviors like scrolling, clicking, and typing.

52. Because Plaintiffs were filling out a form on Noom's website, they both believed that they were only communicating with Noom, and only intended to provide their information and interactions to Noom. They did not believe, nor did they intend, to provide their information and electronic communications to other entities, at least without proper consent.

53. During those visits, and upon information and belief, the Session Replay feature in FullStory's software captured each of Plaintiffs' keystrokes, mouse clicks, and other electronic communications on the Website, which it then analyzed and compiled into a recording. The FullStory wiretap also captured the date and time of the visits, the duration of the visits, Plaintiffs' IP addresses, their locations at the time of the visits, their browser types, and the operating system on their devices.

54. FullStory's recording of keystrokes, mouse clicks, data entry, and other electronic communications begins the moment a user accesses or interacts with the Website.

55. FullStory itself captures, stores, and analyzes electronic communications with the Website. FullStory provides recordings of these communications to Noom, but FullStory itself—an unintended recipient of the communications—still has access to that data.

56. FullStory has repeatedly stated that it is "a party" to any communications captured by its technology, both within its motions to dismiss in this case and elsewhere. Hence, it has repeatedly admitted that it accessed communications. For example, on December 14, 2020, in the matter *Saleh v. Nike, Inc. et al.*, Case No. 2:20-cv-09581, ECF No. 19, at 2:14, FullStory stated it "fit within the well-recognized party exception under CIPA."; *see also id*. at 12 ("FullStory cannot be considered a third party to Plaintiff's communications."). On January 22, 2021, in the matter *Saleh v. Nike, Inc. et al.*, Case No. 2:20-cv-09581, ECF No. 30 at 2:20-22, FullStory stated it was "the recipient[] of Plaintiff's communications and thus fit within CIPA's well-recognized party exception."; *see id*. at 2:20-21 ("FullStory was not a third party to the communication"). On February 19, 2021, in the matter *Saleh v. Nike, Inc. et al.*, Case No. 2:20-cv-09581, ECF No. 32 at 6:8-10, FullStory stated it was "a party to Plaintiff's communication and thus fit within the well-recognized party exception."

57. Similarly, on January 29, 2021, in the matter *Johnson v. Blue Nile, Inc.*, *et al.*, Case No. 3:20-cv-08183-LB, ECF No. 33 at 2:20-23, FullStory stated it "fit within CIPA's well-recognized party exception." On March 4, 2021, in the matter *Johnson v. Blue Nile, Inc.*, *et al.*, Case No. 3:20-cv-08183-LB, ECF No. 37 at 2:22-23, FullStory stated it "fit within CIPA's well-recognized party exception." On March 25, 2021, in the matter of *Johnson v. Blue Nile, Inc.*, *et al.*, Case No. 3:20-cv-08183-LB, ECF No. 41 at 8:10-17, FullStory stated it was "a party to Plaintiff's purported communications."

58. When users access Defendant Noom's website, they fill out a form and enter PII and PHI. FullStory's software captures these electronic communications throughout each step of the process. Even if users do not complete the form, the Website nonetheless captures users' electronic communications throughout his or her visit.

59. On Noom's website, FullStory's software captures, among other things:

(a) The user's height and weight;

(b) The user's gender;

(c) The user's age range;

(d) The user's diet and exercise habits;

(e) Whether the user has "significant back issues";

(f) Whether the user has any of a handful of medical conditions

(g) Whether the user has ever been "diagnosed with or received treatment for diabetes";

(h) The user's email;

(i) The user's IP address;

(j) The user's their location at the time of the visit; and

(k) The user's browser type and the operating system on their devices

60. Crucially, Defendant Noom does not ask users, including Plaintiffs, whether they consent to being wiretapped by FullStory. Users are never told that their electronic communications are being wiretapped by FullStory.

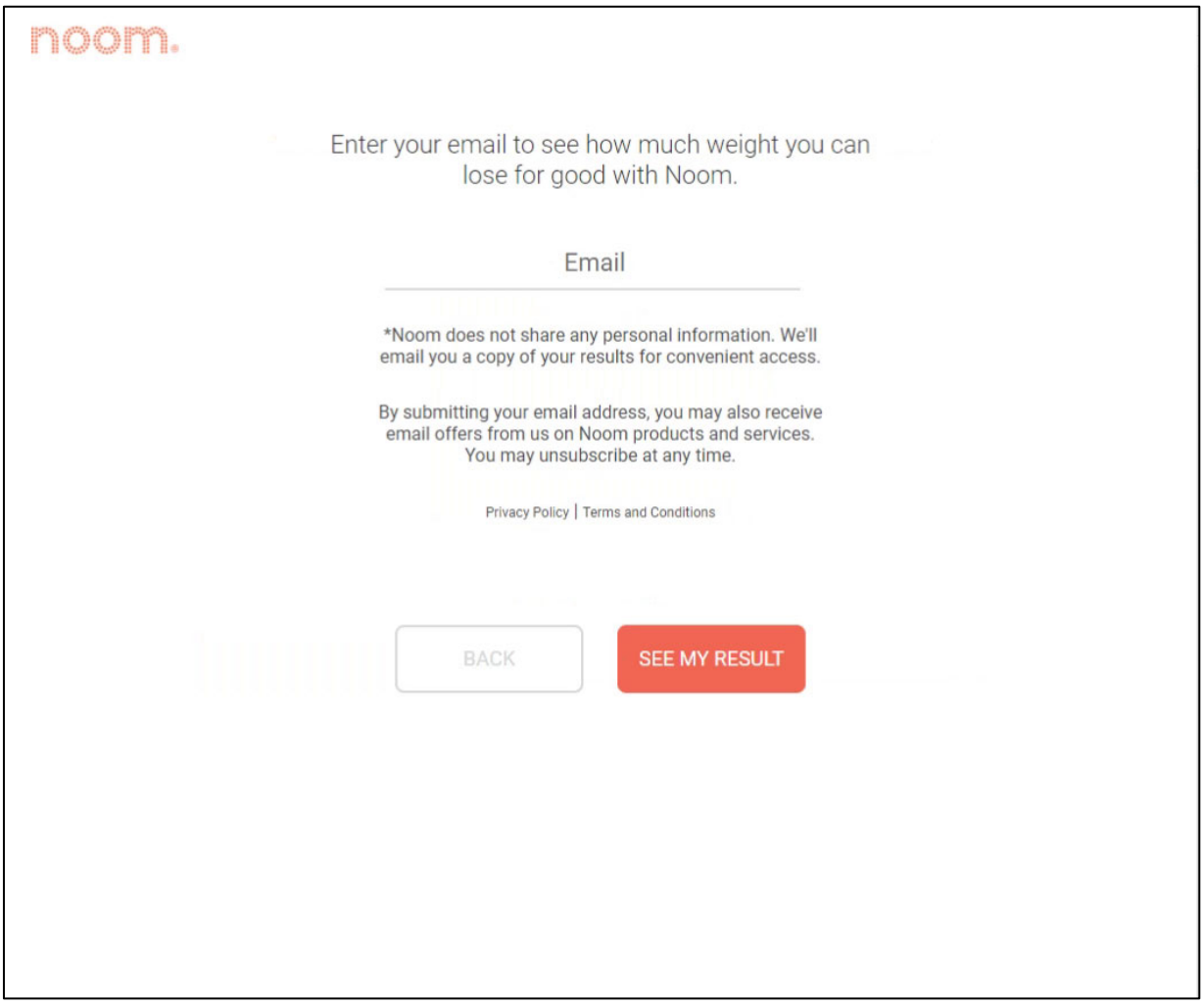
61. Noom's Privacy Policy did not disclose the wiretapping for two reasons. First, to the extent Noom's home page contained a link to the Privacy Policy, it was buried at the very bottom of the webpage in small, non-contrasting font (i.e., light grey against a white background) that was designed to be unobtrusive and easy to overlook. Visitors to the website are given no notice and are not prompted to take any affirmative action to demonstrate assent. Visitors are not required to read or acknowledge the Privacy Policy to use the website. In any event, by the time a website user visited the Privacy Policy, the wiretap on Noom's website will have already deployed.

62. Second, when a user begins using Noom's website and providing personal information, such as weight loss goals, age and weight, etc., the hyperlink to Defendant's Privacy Policy disappears until the end of the form on the Website, *i.e. after* the wiretap has already been deployed. Even then, users are never given the option to accept the Privacy Policy by clicking a button. Noom does not say that by clicking "See My Result," users accept the Privacy Policy; in fact, Noom never tells users *how* to accept the Privacy Policy. And even if a user passively accepts the Privacy Policy by using the Website—which users do not—this purported consent is invalid because users are not shown a link to the Privacy Policy until *after* their privacy has already been breached by the wiretap.

63. Indeed, FullStory cautions its clients to "audit your own site and ensure all appropriate form fields or elements are excluded before you start recording (or that you're recording *only after you have consent*)."

64. Therefore, users like Plaintiffs never agree or are never given the option to agree to the Privacy Policy when using the Website.

65. In addition, the hyperlink to the Privacy Policy—which, again, is not displayed until the end of the form—is in the smallest text on the screen, not underlined, is not the typical color for a hyperlink, is not in all caps, and is surrounded by much more obvious and distracting features, such as the large orange "See My Result" button. These issues are displayed in the below screenshot of the Website:



66. Users, including Plaintiffs, are thus not on notice of the Privacy Policy when they click "See My Result."

67. Second, even if users do agree to the Privacy Policy by using the Website or otherwise—and they do not for the reasons stated above—Noom's Privacy Policy does not mention FullStory or its Session Replay feature in Noom's Privacy Policy. At best, the Privacy Policy consists of vague generalities and disclosures that the website "may" use certain general information such as a user's IP address or operating system, or "may" use various available data collection technologies. Disclosing that Noom has the *capacity* to monitor certain information is not the same as seeking consent to record keystrokes, mouse clicks and other communications in real time.

68. Further, Noom misrepresents certain aspects of its Privacy Policy. For instance,

Noom states in the "Embedded Scripts" section that *if* an Embedded Script is used (the Privacy Policy does not say either way), then "[t]he code is temporarily downloaded onto User's Device from Noom's web server and/or Mobile App or a third party service provider, is active only while User is connected to the Website and/or Mobile App, and is deactivated or deleted thereafter." But the code is not "deactivated or deleted." As FullStory notes on its website:

> If the user navigates away or closes their tab—which is normal behavior—FullStory bundles these events together into a "swan song" bundle, that is, a last ditch attempt to send the event data to FullStory before the page closes. **In some instances, the swan song isn't successful, so the data is stored locally in the user's browser, and the next time the user on that particular device visits the customer's site, the FullStory script will send the swan song data that weren't successfully sent on the user's last visit.** These swan song events will be processed and appear as part of the original FullStory session.[10]

69. In addition, as the 2017 Princeton University study researchers recognized, "the extent of data collected by these services **far exceeds user expectations** [1]; text typed into forms is collected before the user submits the form, and precise mouse movements are saved, all without any visual indication to the user. This data can't reasonably be expected to be kept anonymous." Thus, a reasonable user reviewing Noom's Privacy Policy would not expect it to allow the real-time recording of said user's actions on the Website.

70. The language in Noom's Privacy Policy is also a far cry from how FullStory encourages its partners to disclose the use of its technology:

> If you are a Visitor, FullStory collects information on your use of the Site, such as pages visited, links clicked, non-sensitive text entered, and mouse movements, as well as information more commonly collected such as the referring URL, browser, operating system, and Internet Protocol ("IP") address.

71. Indeed, unlike Noom, other companies actively disclose the use of session recording technology on their websites by implementing a pop-up screen that a user must acknowledge before advancing further on the website. That practice goes to show that companies know how to disclose the use of session recording technology when they want to.

72. Neither Plaintiffs nor any Class member consented to being wiretapped on the

[10] https://help.fullstory.com/hc/en-us/articles/360048109714-Swan-songs-How-FullStory-records-sessions-that-end-unexpectedly (emphasis added).

Website, or to have their communications recorded and shared with FullStory. Any purported consent that was obtained was ineffective because (i) the wiretapping began from the moment Plaintiffs and Class members accessed the Website; (ii) the Privacy Policy did not disclose the wiretapping or FullStory; (iii) Plaintiffs and Class members are not given the option to accept the Privacy Policy, or told how they can accept it; and (iv) the hyperlink to the Privacy Policy is inconspicuous and therefore insufficient to provide notice.

73. In short, when Plaintiffs and other Class members accessed Noom's website, their electronic communications with Noom—which were only intended for Noom—were surreptitiously captured, stored, and analyzed by FullStory, who was not an intended party to these communications. Unlike a simple cookie, FullStory's software does far more than simply track where a visitor went on the internet. And unlike a simple tape recorder or screen recorder, the data FullStory captures leaves the "Noom ecosystem" because FullStory—an unintended "third party auditor" to Plaintiffs' communications—has access to the communications, can analyze those communications, and can combine those communications with other data it receives from Noom (and thus has access to said extraneous data). Such software not only allows FullStory, as enabled by Noom, to build a comprehensive image of users, it constitutes wiretapping. Noom also did not obtain proper consent from users, and did not properly disclose FullStory in its Privacy Policy.

CLASS ACTION ALLEGATIONS

74. Plaintiffs seek to represent a class of all California residents who visited Noom.com, and whose electronic communications were intercepted or recorded by FullStory. Plaintiffs reserve the right to modify the class definition as appropriate based on further investigation and discovery obtained in the case.

75. Members of the Class are so numerous that their individual joinder herein is impracticable. On information and belief, members of the Class number in the thousands. The precise number of Class members and their identities are unknown to Plaintiffs at this time but may be determined through discovery. Class members may be notified of the pendency of this action by mail and/or publication through the distribution records of Defendants.

76. Common questions of law and fact exist as to all Class members and predominate over questions affecting only individual Class members. Common legal and factual questions include, but are not limited to, whether Defendants have violated the California Invasion of Privacy Act ("CIPA"), Cal. Penal Code § 631 and invaded Plaintiffs' privacy rights in violation of the California Constitution; and whether class members are entitled to actual and/or statutory damages for the aforementioned violations.

77. The claims of the named Plaintiffs are typical of the claims of the Class because the named Plaintiffs, like all other class members, visited the Website and had their electronic communications intercepted and disclosed to FullStory through the use of FullStory's wiretaps.

78. Plaintiffs are adequate representatives of the Class because their interests do not conflict with the interests of the Class members they seek to represent, they have retained competent counsel experienced in prosecuting class actions, and they intend to prosecute this action vigorously. The interests of Class members will be fairly and adequately protected by Plaintiffs and their counsel.

79. The class mechanism is superior to other available means for the fair and efficient adjudication of the claims of Class members. Each individual Class member may lack the resources to undergo the burden and expense of individual prosecution of the complex and extensive litigation necessary to establish Defendants' liability. Individualized litigation increases the delay and expense to all parties and multiplies the burden on the judicial system presented by the complex legal and factual issues of this case. Individualized litigation also presents a potential for inconsistent or contradictory judgments. In contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court on the issue of Defendants' liability. Class treatment of the liability issues will ensure that all claims and claimants are before this Court for consistent adjudication of the liability issues.

80. Plaintiffs bring all claims in this action individually and on behalf of members of the Class against Defendants.

COUNT I
Violation Of The California Invasion Of Privacy Act,
Cal. Penal Code § 631

81. Plaintiffs repeat the allegations contained in the foregoing paragraphs as if fully set forth herein.

82. Plaintiffs bring this claim individually and on behalf of the members of the proposed Class against Defendants.

83. To establish liability under section 631(a), Plaintiffs need only establish that Defendants, "by means of any machine, instrument, contrivance, or in any other manner," did any of the following:

> Intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system,
>
> *Or*
>
> Willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads or attempts to read or learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line or cable or is being sent from or received at any place within this state,
>
> *Or*
>
> Uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained,
>
> *Or*
>
> Aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section.

84. Section 631(a) is not limited to phone lines, but also applies to "new technologies" such as computers, the Internet, and email. *See Matera v. Google Inc.*, 2016 WL 8200619, at *21 (N.D. Cal. Aug. 12, 2016) (CIPA applies to "new technologies" and must be construed broadly to effectuate its remedial purpose of protecting privacy); *Bradley v. Google, Inc.*, 2006 WL 3798134, at *5-6 (N.D. Cal. Dec. 22, 2006) (CIPA governs "electronic communications"); *In re Facebook,*

Inc. Internet Tracking Litigation, 956 F.3d 589 (9th Cir. 2020) (reversing dismissal of CIPA and common law privacy claims based on Facebook's collection of consumers' Internet browsing history).

85. The California Supreme Court has twice explained that the "express objective" of CIPA is to "protect a person placing or receiving a call from a situation where the person on the other end of the line permits an outsider to tap his telephone or listen in on the call." *Ribas v. Clark*, 38 Cal. 3d 355, 364 (1985); *Smith v. LoanMe*, --- P.3d --- 2021 WL 1217873, at *8 (Cal. April 1, 2021) ("As [the California Supreme Court] explained in *Ribas* … a substantial distinction has been recognized between the secondhand repetition of the contents of a conversation and its simultaneous dissemination to an unannounced second auditor, whether that auditor be a person or mechanical device."). The Ninth Circuit similarly explained that one of the purposes of wiretapping statutes is "to prevent the acquisition of the contents of a message by an unauthorized third-party or 'an unseen auditor.'" *In re Facebook Internet Tracking Litig.*, 956 F.3d at 608.

86. FullStory's software, including its Session Replay feature, is a "machine, instrument, contrivance, or … other manner" used to engage in the prohibited conduct at issue here.

87. At all relevant times, by using FullStory's technology, FullStory intentionally tapped, electrically or otherwise, the lines of internet communication between Plaintiffs and class members on the one hand, and Noom's Website on the other hand.

88. At all relevant times, by using FullStory's technology, FullStory willfully and without the consent of all parties to the communication, or in any unauthorized manner, read or attempted to read or learn the contents or meaning of electronic communications of Plaintiffs and putative Class members, while the electronic communications were in transit or passing over any wire, line or cable or were being sent from or received at any place within California.

89. The actionable "content" at issue here falls under two categories. The first category involves the webpages and URLs that Plaintiffs viewed while on the website. The second covers Plaintiffs' keystrokes, mouse clicks, form field entries, and any other information Plaintiffs intentionally provided to Noom while on the website. These categories include the webpages that

Plaintiffs saw, and the information they provided on each webpage, when Noom asked for information about the Plaintiffs.

90. As FullStory notes on its website, "When an end user session is recorded by the FullStory script, FullStory starts by recording event data locally in the browser. Every few seconds, this local event data is packaged up and sent to FullStory recording servers in the form of bundles." Such local recording is plainly occurring in real-time, and is, at worst, "transitory electronic storage" that is "part of the overall transmission process," which has been held to constitute communications "in transit."

91. Noom aided, agreed with, and conspired with FullStory to implement FullStory's technology on its website, thus enabling FullStory to intercept, capture, store, analyze, and otherwise wiretap the electronic communications of Plaintiffs and Class Members with Noom's Website, without proper consent.

92. Plaintiffs and Class Members did not consent to any of Noom's actions in enabling FullStory wiretap visitors to the Website. Nor have Plaintiffs or Class Members consented to FullStory's intentional access, interception, reading, learning, recording, and collection of Plaintiffs and Class Members' electronic communications.

93. The violation of section 631(a) constitutes an invasion of privacy sufficient to confer Article III standing.

94. Unless enjoined, Defendants will continue to commit the illegal acts alleged here. Plaintiffs continue to be at risk because they frequently use the internet to search for information about products or services. They continue to desire to use the internet for that purpose, including for the purpose of shopping for various diets, weight loss plans, or other health-related products. Defendant FullStory provides its software, including the Session Replay feature, to many other website operators who offer a wide array of services. For many websites that Plaintiffs may or are likely to visit in the future, they have no practical way to know if their website communications will be monitored or recorded by FullStory.

95. Plaintiffs and Class Members seek all relief available under Cal. Penal Code § 637.2, including statutory damages of $5,000 per violation.

96. Plaintiff Moise also seeks injunctive relief. Plaintiff Moise was interested in using Noom's weight loss program, but was perturbed by the surreptitious collection of data by FullStory. Plaintiff Moise would be willing to use Noom's program if she knew that she would not be wiretapped by FullStory when she provided her personal information.

COUNT II
Violation Of The California Invasion Of Privacy Act,
Cal. Penal Code § 635

97. Plaintiffs repeat the allegations contained in the foregoing paragraphs as if fully set forth herein.

98. Plaintiffs bring this claim individually and on behalf of the members of the proposed Class against Defendants.

99. California Penal Code § 635 provides, in pertinent part:

> Every person who manufactures, assembles, sells, offers for sale, advertises for sale, possesses, transports, imports, or furnishes to another any device which is primarily or exclusively designed or intended for eavesdropping upon the communication of another, or any device which is primarily or exclusively designed or intended for the unauthorized interception or reception of communications between cellular radio telephones or between a cellular radio telephone and a landline telephone in violation of Section 632.5, or communications between cordless telephones or between a cordless telephone and a landline telephone in violation of Section 632.6 , shall be punished by a fine not exceeding two thousand five hundred dollars.

100. At all relevant times, FullStory intentionally manufactured, assembled, sold, offered for sale, advertised for sale, transported, imported, and/or furnished a wiretap device that is primarily or exclusively designed or intended for eavesdropping upon the communication of another.

101. At all relevant times, by enabling FullStory to wiretap visitors to its Website, Noom possessed and used a wiretap device that is primarily or exclusively designed or intended for eavesdropping upon the communication of another.

102. FullStory's code is a "device" that is "primarily or exclusively designed" for eavesdropping. That is, the FullStory's code is designed to gather PII, keystrokes, mouse clicks, and other electronic communications.

103. Plaintiffs and Class Members did not consent to Noom's actions in enabling Fullstory to wiretap visitors to the Website, nor did they consent to FullStory wiretapping their electronic communications.

104. Unless enjoined, Defendants will continue to commit the illegal acts alleged here. Plaintiffs continue to be at risk because they frequently use the internet to search for information about products or services. They continue to desire to use the internet for that purpose, including for the purpose of shopping for various diets, weight loss plans, or other health-related products. Defendant FullStory provides its software, including the Session Replay feature, to many other website operators who offer a wide array of services. For many websites that Plaintiffs may or are likely to visit in the future, they have no practical way to know if their website communications will be monitored or recorded by FullStory.

105. The violation of section 635 constitutes an invasion of privacy sufficient to confer Article III standing.

106. Plaintiffs and Class Members seek all relief available under Cal. Penal Code § 637.2, including statutory damages of $5,000 per violation.

107. Plaintiff Moise also seeks injunctive relief. Plaintiff Moise was interested in using Noom's weight loss program, but was perturbed by the surreptitious collection of data by FullStory. Plaintiff Moise would be willing to use Noom's program if she knew that she would not be wiretapped by FullStory when she entered her personal information on the Website.

COUNT III
Invasion Of Privacy Under California's Constitution

108. Plaintiffs repeat the allegations contained in the foregoing paragraphs as if fully set forth herein.

109. Plaintiffs bring this claim individually and on behalf of the members of the proposed Class against Defendants.

110. Plaintiffs and Class Members have an interest in: (1) precluding the dissemination and/or misuse of their sensitive, confidential PII and PHI; and (2) making personal decisions and/or conducting personal activities without observation, intrusion or interference, including, but not limited to, the right to visit and interact with various Internet sites without being subjected to wiretaps without Plaintiffs' and Class Members' knowledge or consent.

111. At all relevant times, by implementing FullStory's wiretaps on Noom's Website, each Defendant intentionally invaded Plaintiffs' and Class Members' privacy rights under the California Constitution, and procured the other Defendant to do so.

112. Plaintiffs and Class Members had a reasonable expectation that their PII, PHI, and other data would remain confidential and that Defendants would not install wiretaps on the Website.

113. Plaintiffs and Class Members did not consent to any of Defendants' actions in implementing FullStory's wiretaps on the Website.

114. This invasion of privacy is serious in nature, scope and impact.

115. This invasion of privacy alleged here constitutes an egregious breach of the social norms underlying the privacy right.

116. Plaintiffs and Class Members seek all relief available for invasion of privacy claims under California's Constitution.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all others similarly situated, seek judgment against Defendants, as follows:

(a) For an order certifying the Class under Rule 23 and naming Plaintiffs as the representatives of the Class and Plaintiffs' attorneys as Class Counsel to represent the Class;

(b) For an order declaring that the Defendants' conduct violates the statutes referenced herein;

(c) For an order finding in favor of Plaintiffs and the Class on all counts asserted herein;

(d) For compensatory, punitive, and statutory damages in amounts to be determined by the Court and/or jury;

(e) For prejudgment interest on all amounts awarded;

(f) For injunctive relief as pleaded or as the Court may deem proper; and

(g) For an order awarding Plaintiffs and the Class their reasonable attorneys' fees and expenses and costs of suit.

DEMAND FOR TRIAL BY JURY

Plaintiffs demand a trial by jury of all issues so triable.

Dated: April 29, 2021

Respectfully submitted,

BURSOR & FISHER, P.A.

By: /s/ *Joel D. Smith*
Joel D. Smith

L. Timothy Fisher (State Bar No. 191626)
Joel D. Smith (State Bar No. 244902)
1990 North California Boulevard, Suite 940
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
E-Mail: ltfisher@bursor.com
jsmith@bursor.com

BURSOR & FISHER, P.A.
Alec M. Leslie (*Pro Hac Vice*)
Max S. Roberts (*Pro Hac Vice*)
888 Seventh Avenue, Third Floor
New York, NY 10019
Telephone: (646) 837-7150
Facsimile: (212) 989-9163
E-Mail: aleslie@bursor.com
mroberts@bursor.com

Attorneys for Plaintiffs